

The opinion in support of the decision being entered today was *not* written for publication and is *not* binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte JOHN OWLETT

Appeal 2007-0644
Application 10/081,500
Technology Center 2100

Decided: June 20, 2007

Before KENNETH W. HAIRSTON, LANCE LEONARD BARRY,
and HOWARD B. BLANKENSHIP, *Administrative Patent Judges*.

BLANKENSHIP, *Administrative Patent Judge*.

DECISION ON APPEAL

This appeal involves claims 1-14, the only claims pending in this application. We have jurisdiction under 35 U.S.C. §§ 6(b), 134(a).

INTRODUCTION

The claims relate to a method and system for authentication of a user by an authenticating entity. The authenticating entity sends a challenge (e.g., a bit sequence) to the user, to which the user adds a spoiler (e.g., an additional bit sequence). The user encrypts the combined spoiler and challenge using a private key of an asymmetric key pair. Claim 1 is illustrative:

1. A method for authentication of a user by an authenticating entity comprising the steps of:

the authenticating entity sending a challenge to the user;

the user adding a spoiler to the challenge;

the user encrypting the combined spoiler and challenge using a private key of an asymmetric key pair;

the user sending a response to the authenticating entity in the form of the encrypted combined spoiler and challenge.

The Examiner relies on the following prior art references to show unpatentability:

Tsudik	US 6,072,875	Jun. 6, 2000
Andersson	US 2002/0034301 A1	Mar. 21, 2002
Hara	US 2004/0202328 A1	Oct. 14, 2004

The rejections as presented by the Examiner are as follows:

1. Claims 1-5 and 11-14 are rejected under 35 U.S.C. § 103(a) as unpatentable over Andersson and Hara.
2. Claims 6-10 are rejected under 35 U.S.C § 103(a) as unpatentable over Andersson, Hara, and Tsudik.

OPINION

We select claim 1 as representative of independent claims 1, 13, and 14. Further, we will consider dependent claims to the extent that Appellant provides separate arguments for the claims. *See* 37 C.F.R. § 41.37(c)(1)(vii).

The Examiner finds that Andersson teaches (e.g., ¶ 40) the subject matter of representative claim 1, except for the user adding a spoiler to the challenge and encrypting the combined spoiler and challenge. The Examiner turns to Hara, which discloses (¶¶ 83-84) padding of an IP datagram to make the length of a data part an integer multiple of 64 bits. According to Hara, the data part is then better suited for encryption. The Examiner concludes that it would have been obvious to pad the data for encryption in the method described by Andersson.

Appellant submits, however, that the proposed combination fails to meet the requirements of claim 1. In Appellant's view, the "padding" described by Hara cannot be considered a "spoiler" as recited in the claim. (Br. 5-9; Reply Br. 2-4.)

Appellant's Specification teaches that the "spoiler" may be added to the challenge as a prefix or a suffix. (Specification 8: 1-4.) "The challenge may be a bit sequence. The spoiler may be an additional bit sequence." (*Id.* at ll. 20-21.)

Contrary to the implications of Appellant's arguments, we do not find that the Specification teaches that the "additional bit sequence" of the spoiler cannot consist entirely of "1" bits (i.e., in accordance with the teachings of Hara with respect to the "padding" of bits). Appellant argues, without

citation to any authority or other evidence, that a “spoiler” consisting of “1” bits would provide inadequate security. We reject Appellant’s unfounded allegation, without more. In accordance with the teachings of Hara (and in accordance with instant claim 1), the additional bit sequence is encrypted, along with the message portion of the datagram (e.g., the challenge bit sequence), prior to transmission. After encryption, the bits residing in the original bit positions of the padding (or spoiler) would not likely be identical to the bits before the encryption, contrary to the apparent premise of Appellant’s argument.

Even were we to accept the premise that a “spoiler” consisting of “1” bits would provide less security than that intended by Appellant, Appellant does not argue that a spoiler consisting of “1” bits would render the claimed invention inoperative. At best, Appellant argues that such a spoiler would compromise system security to some extent when compared with, for example, a spoiler consisting of a random sequence of bits. However, instant claim 1 does not, by its terms, distinguish over a spoiler consisting of bits such as those taught by Hara. Nor does the claim provide any other indication of how system security may be either strengthened or compromised by selection of a spoiler bit sequence. For example, the claim is not as specific as the “some embodiments” argued at page 3 of the Reply Brief, where the spoiler value must be shared with another user for the purposes of decrypting a communication. That a better selection of bits for a spoiler might be indicated than the sequence taught by Hara is simply not material, in view of the broad scope of the claim. “What matters is the objective reach of the claim. If the claim extends to what is obvious, it is

invalid under §103.” *KSR Int’l Co. v. Teleflex, Inc.*, 127 S. Ct. 1727, 1741, 82 USPQ2d 1385, 1397.

We also disagree with Appellant that the Examiner’s finding of a motivation to combine the references is not “clear and particular.” The finding is based on the express teachings of Hara; i.e., adding bits to a message facilitates encryption, especially types of encryption suited for high-speed transmission of data. Appellant’s point may be there is no teaching in the references to add bits to a challenge, before encryption and transmission, for the particular purpose taught by Appellant. We can agree to the extent that Appellant’s purpose is not in the applied prior art, but the reason for the combination need not be the same as that of Appellant’s. “In determining whether the subject matter of a patent claim is obvious, neither the particular motivation nor the avowed purpose of the patentee controls.” *KSR*, 127 S. Ct. at 1741-42, 82 USPQ2d at 1397.

The Examiner adds Tsudik to the teachings of Andersson and Hara in the § 103(a) rejection of claims 6 through 10. Instant claim 6 recites that the method of claim 1 further includes the user obtaining a digest of the combined spoiler and challenge before the step of encrypting. Appellant argues (Br. 10-11) that nothing in column 3, line 59 to column 4, line 11 of Tsudik discloses or suggests the digest recitation.

Tsudik in the referenced section describes securing information by encrypting the information using a “secret one-way function.” The one-way function may be a prior art message digest algorithm, according to column 5,

lines 60 through 66 of Tsudik.¹ We are thus not persuaded that the combined teachings of Andersson, Hara, and Tsudik fail to teach or suggest the additional step of obtaining a digest as claimed. Moreover, Appellant's Specification admits (e.g., at 3: 14-24; Fig. 1) that digests were conventional in the art to reduce processing and communication overheads.

We have considered all of Appellant's arguments in support of representative claims 1 and 6, but find no error in their rejection. Claims 2-5, 7, 8, and 10-14 fall with claims 1 and 6.

Instant claim 9 recites that the method of claim 1 further includes that the user sends details of the algorithm used for encryption to the authenticating entity. The rejection (Answer 6) refers to column 5, lines 27 through 48 of Tsudik for the teaching. That section of Tsudik teaches that a user, when travelling to a foreign domain, must not only be authenticated but also identified to the foreign domain. The identity of the user must also be communicated to the home domain authority.

We agree with Appellant (Br. 11) that the cited portions of Tsudik do not disclose or suggest the algorithm recitation of claim 9. The Examiner has not provided the article ("Molva") describing authentication of a user that Tsudik incorporates by reference at column 5, lines 38 through 40; we conclude that the rejection does not rely on any details of the Molva article that cannot be found within Tsudik. Further, the Examiner has not provided any evidence that it was conventional in the art to send details of the

¹ Tsudik refers to the "MD5" algorithm as disclosed by Rivest, which is item 9, not item 7, in the references listed in column 3 of Tsudik.

algorithm used for encryption to the authenticating entity. We thus do not sustain the rejection of claim 9.

CONCLUSION

The rejection of claims 1-5 and 11-14 under 35 U.S.C. § 103(a) as unpatentable over Andersson and Hara is affirmed. The rejection of claims 6-10 under 35 U.S.C § 103(a) as unpatentable over Andersson, Hara, and Tsudik is affirmed with respect to claims 6-8 and 10, but reversed with respect to claim 9. The Examiner's decision is thus affirmed-in-part.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a).

AFFIRMED-IN-PART

KIS

MYERS, BIGEL, SIBLEY & SAJOVEC, P.A.
P. O. BOX 37428
RALEIGH, NC 27627